Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Analyse en droit comparé des réglementations de protection des données personnelles

de Terwangne , Cécile

Published in:
Journal de Réflexion sur l'Informatique

Publication date:
1990

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
de Terwangne , C 1990, 'Analyse en droit comparé des réglementations de protection des données personnelles', *Journal de Réflexion sur l'Informatique*, Numéro 17, p. 37-40.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 06. May. 2023

Analyse en droit comparé des réglementations de protection des données personnelles

Dans sa grande majorité, l'Europe se sent concernée par le danger que représente pour la vie privée le traitement automatisé de données personnelles. Il y a plus de quinze ans déjà, la Suède, pionnière, adoptait son «Data Act», loi visant à protéger les données nominatives.

Apparaissaient ensuite les premiers textes de loi en Allemagne en 1977, en France, en Autriche, au Danemark et en Norvège en 1978, au Luxembourg en 1979. Le Conseil de l'Europe a également fait montre de diligence en la matière, puisqu'en 1981 il élaborait une convention et la proposait à la signature des Etats [1]. Le mouvement législatif ainsi entamé s'est poursuivi jusqu'à nos jours, conduisant l'Islande (en 1982), le Royaume-Uni (1984), l'Irlande et les Pays-Bas (1988) à se doter à leur tour d'un régime légal de protection des données.

Notre propos s'attachera à décrire, dans une approche comparée, les grandes lignes de ces différentes législations, en incluant dans son champ les projets de loi en voie d'adoption en Grèce, au Portugal et, tout récemment, en Belgique [2].

Champ d'application des réglementations

Si l'objet de l'ensemble des législations étudiées porte d'une même manière sur l'instauration d'un régime légal de protection des données personnelles, le champ d'application des différents textes varie sensiblement d'une version à l'autre.

Il peut ainsi - comme c'est le cas dans la majorité des Etats - ne pas être limité aux seuls *traitements automatisés de données*, et s'étendre à certains *fichiers manuels*. Les législations anglaise et irlandaise, de même que le projet de loi portugais, s'avèrent être les seuls à ne pas s'appliquer d'une manière ou d'une autre à ceux-ci.

La protection légale peut également, au-delà des données relatives à des *individus*, s'attacher aux informations concernant les personnes morales. Seuls le Danemark, le Luxembourg, l'Autriche, l'Islande et la Norvège ont opté jusqu'ici pour l'extension de leurs régimes protecteurs aux *personnes morales*.

Une catégorie de données bénéficie d'une attention particulière de la part des législateurs. Ces derniers ont chacun apporté une réponse différente tant dans leur définition du contenu de cette catégorie de *données dites «sensibles»* que dans le régime accordé à ces données. Le Royaume-Uni, l'Irlande et les Pays-Bas prévoient une protection accrue pour les données personnelles intimes. La loi française, quant à elle, interdit l'enregistrement de telles données sans le consentement exprès de la personne à laquelle les données se rapportent. Les législations luxembourgeoise et danoise en prohibent l'enregistrement excepté dans certaines circonstances. Enfin, en radicale opposition, les législateurs allemand et autrichien n'admettent pas de distinction qualitative entre les données et, dès lors, ne reconnaissent pas le concept même de «données sensibles» alors que la Grèce distingue trois sortes de données nominatives: les données strictement personnelles, les données confidentielles et les données personnelles.

Les exceptions au champ d'application des lois ne procèdent pas partout de la même logique. Certaines réglementations excluent les traitements effectués par les entreprises de presse pour leurs objectifs journalistiques (R.F.A., Pays-Bas et Autriche). D'autres considèrent les besoins de sécurité de l'Etat et exemptent des dispositions légales les fichiers tenus à cette fin (Pays-Bas, Irlande, Royaume-Uni, Autriche). Les traitements de données statistiques sont également hors du champ de diverses législations (Danemark, R.F.A.,Norvège, Pays-Bas, Belgique). Enfin, certains législateurs ont jugé bon de dispenser des diverses obligations légales les fichiers tenus à des fins privées, familiales ou même récréatives (Irlande, Royaume-Uni, Pays-Bas, Belgique), de même que les fichiers contenant des données ayant déjà fait l'objet d'une publicité en vertu d'autres dispositions légales (Irlande, Royaume-Uni, Belgique et France - non aux termes mêmes de la loi française mais bien en accord avec l'interprétation de la CNIL).

Principes de base

Collecte et enregistrement des données

Les tenants de la protection des données mettent davantage l'accent sur le caractère adéquat du traitement effectué sur les informations nominatives que sur la nécessité de prévenir la collecte de données qui ne présenteraient qu'un intérêt marginal face aux besoins et finalités de l'organisme collecteur. Les données sensibles n'entrent toutefois pas dans le

champ de cette remarque, les législateurs ayant été attentifs à déterminer les critères de légitimité de leur collecte aussi bien que de leur traitement.

La Convention du Conseil de l'Europe se réfère implicitement à la collecte de données lorsque, dans son article 5, elle énonce que les données personnelles doivent être *«obtenues loyalement et licitement»*. Il découle de l'esprit du texte que, là où cela est possible, les informations doivent être obtenues directement de la personne concernée.

Si certains Etats ont intégré en termes fidèles la disposition de l'article 5 à leur législation interne (tels le Royaume-Uni, l'Irlande, le Luxembourg ou la France), la plupart ne font pas mention de la collecte de façon explicite et recourent à la seule règle de la pertinence des données enregistrées. Cette règle est présente dans la large majorité des réglementations. L'expression n'est pas identique mais les termes sont nettement similaires.

Ainsi, à titre d'exemple, la loi danoise pose qu'une *«entreprise est autorisée à collecter des données seulement dans la mesure où l'enregistrement des données est partie naturelle des opérations normales de l'entreprise»*, la loi norvégienne, pour sa part, stipule que *«l'enregistrement des informations personnelles doit être justifié au regard des activités administratives ou opérationnelles de l'entreprise»*.

Etant donné l'interrelation étroite entre, d'une part, la finalité poursuivie lors de la collecte des données, d'autre part, l'enregistrement et l'utilisation de ces dernières, la règle de la pertinence doit être envisagée dans une lecture conjointe avec le principe de finalité, principe fondamental à l'analyse duquel il y a lieu de s'attacher à présent.

Définitions des finalités

Une des règles cardinales en matière de protection des données réside dans le fait que tout fichier doit être créé et utilisé en vue de finalités spécifiques et définies. Les législateurs sont unanimes à reprendre le principe. Chacune des lois nationales étudiées, en effet, soit requiert la détermination des objectifs poursuivis lors de la procédure d'enregistrement, soit conditionne la collecte et l'utilisation des données personnelles à l'absence de violation d'intérêts privés, soit encore édicte les deux exigences, ce qui est d'ailleurs le plus souvent le cas. La Convention du Conseil de l'Europe requiert également que le but du traitement soit spécifié.

Ainsi l'obligation de définir la finalité poursuivie, *per se*, est devenue une norme de protection des données. Les textes cependant n'établissent pas d'une manière aussi éclairante les critères qui devraient permettre aux autorités de contrôle de décider de la légitimité des finalités avancées et partant, de leur recevabilité. Deux approches se dessinent dans la législation :

- les finalités poursuivies doivent présenter un lien étroit avec les activités du maître du fichier (e.a. Royaume-Uni et Danemark);
- les objectifs ne doivent pas conduire à léser les intérêts personnels d'individus fichés (e.a. Autriche, Norvège, Suède).

La France et le Luxembourg ne relient pas la finalité du traitement à l'utilisation légitime des données, mais cela se retrouve de façon implicite dans leur législation respective. La R.F.A. et l'Islande envisagent les finalités en rapport avec les relations contractuelles ou directes établies avec les personnes auxquelles les données traitées se rapportent.

Une des règles cardinales en matière de protection des données réside dans le fait que tout fichier doit être créé et utilisé en vue de finalités spécifiques et définies.

Communication des données à des tiers

Si la transmission de données personnelles à des tiers est autorisée dans l'ensemble des Etats, les dispositions qui s'y appliquent n'en présentent pas moins de nombreuses disparités.

Alors que la solution adoptée par la majorité des Etats est la non-consultation du sujet, aux termes des lois danoise et autrichienne, le consentement préalable de la personne concernée est requis pour la transmission de certaines catégories de données [3]. Certaines législations, notamment néerlandaise et danoise, ont été attentives aux situations où des opérations de mailing direct sont en cause pour imposer des obligations supplémentaires dans ce cas, tandis que d'autres ont pris en compte le devoir de confidentialité qui se rattache à certaines professions ou fonctions et interdisent alors toute communication (lois allemande, néerlandaise, projet portugais).

Les exceptions admises aux dispositions concernant la transmission des données nominatives diffèrent considérablement. Ainsi, si certaines lois exemptent la transmission à des fins scientifiques et statistiques (Danemark, Pays-Bas), d'autres font de même pour la communication de données dans l'intérêt de la répression des infractions ou de la protection de la sécurité de l'Etat (Royaume-Uni, Irlande, Grèce) et d'autres encore soustraient à la protection légale la transmission d'informations limitées aux noms, adresses,...(R.F.A., Pays-Bas).

L'obligation de notifier ultérieurement aux tiers les éventuelles rectifications portant sur les données transmises se rencontre dans les législations fran-

çaise, luxembourgeoise, hollandaise, irlandaise, allemande - découlant de principes administratifs - et belge. Le projet de loi grec prévoit que dès lors qu'une demande de rectification de données est déposée, toute communication de ces données est prohibée. Le Royaume-Uni et le Portugal par contre n'imposent aucune obligation en cas de rectification postérieure à la transmission.

Obligations du «ficheur» et Droits du «fiché»

Autorisation

L'obligation d'obtenir une autorisation avant la création et la mise en oeuvre d'un traitement de données personnelles est intégrée de façon fort variable dans les diverses législations étudiées.

Ni la R.F.A., l'Irlande, le Royaume-Uni, les Pays-Bas, ni la Belgique n'ont inséré une telle obligation dans leur réglementation, alors que la loi luxembourgeoise requiert une autorisation pour *tous* les fichiers personnels, que l'Acte danois en requiert pour les «listes noires», la loi française pour les traitements nominatifs dans le secteur public et le projet de loi grec pour les fichiers contenant des données personnelles.

Enregistrement

Dans la très large majorité des Etats, une procédure d'enregistrement est imposée pour tout fichier contenant des données personnelles. Les exigences des différentes législations ne sont cependant pas uniformes [4].

Certaines réglementations présentent des exigences d'enregistrement très larges, tant par le fait que la formalité est très complète que par celui qu'elle s'impose à tous les maîtres de fichiers (*Act* du Royaume-Uni et projet de loi belge notamment). A l'inverse, certains Etats n'obligent à l'enregistrement que des catégories spécifiques de maîtres de fichiers. C'est le cas de l'Irlande. Ce l'est aussi du Danemark et de l'Islande qui ne requièrent l'enregistrement que des fichiers contenant des informations financières, et de la R.F.A. qui ne l'impose que pour le secteur privé, lorsque les données sont destinées à être transmises à des tiers. Divers législateurs - français, allemand, luxembourgeois et néerlandais - ont distingué selon que les fichiers sont tenus dans le secteur public ou privé.

La France et l'Angleterre ont fait preuve d'originalité en la matière en admettant une version simplifiée de la formalité d'enregistrement. Le *Data Act* britannique autorise en effet l'enregistrement simplifié pour les petites entreprises, et la France fait de même dans les cas où le traitement n'atteint pas, de toute évidence, la vie privée.

Notification de l'existence des fichiers

L'obligation de notifier à une personne concernée l'existence de fichiers contenant des données personnelles, se rencontre dans les lois danoise, allemande, hollandaise, norvégienne et islandaise et dans le projet belge. Les circonstances dans lesquelles une telle obligation doit être respectée sont toutefois différentes. Selon les lois luxembourgeoise et française, l'exigence de notification n'existe pas en soi mais les individus doivent être informés au moment de la collecte de données les concernant. Aucune obligation, enfin, n'existe au Royaume-Uni, en Irlande, en Grèce ni au Portugal.

Droit d'accès, de rectification et de radiation

Toute personne est en droit, les législateurs sont unanimes, de se voir confirmer si des données personnelles la concernant sont contenues dans un fichier et d'obtenir des informations sur la teneur de ces données. La Belgique est le seul Etat à imposer, aux termes de son projet de loi, la gratuité de la communication des renseignements.

Les exceptions légales au droit d'accès sont nombreuses et variées. Les lois néerlandaise et allemande n'en admettent que peu mais précisent par ailleurs, et en cela rejoignent la position danoise, que l'accès peut être refusé s'il devait léser des intérêts dignes de protection (en ce compris les intérêts du maître du fichier).

Le droit de faire rectifier ou d'effacer des données incomplètes, incorrectes ou indûment conservées, est présent dans l'ensemble des législations étudiées. Des spécificités peuvent cependant être observées quant aux circonstances dans lesquelles un tel droit peut être invoqué.

Droit d'action

Les actions ouvertes aux personnes concernées qui ont encouru un dommage sont variables. Dans la plupart des Etats, les sujets peuvent intenter une action ordinaire en responsabilité civile ou contractuelle. Seules les lois néerlandaise et du Royaume-Uni prévoient une action civile spéciale en cette matière. Le *Data Act* britannique, par exemple, reconnaît un droit spécifique à obtenir compensation si les données nominatives sont inexactes et si le sujet est atteint lors de la transmission des données. La loi irlandaise instaure une obligation de diligence dans le chef du maître du fichier, ce qui facilite toute action de la personne concernée.

Organes de contrôle

40 Dans chaque Etat, des autorités de contrôle indépendantes ont été ou doivent être mises en place. Les différents législateurs s'étant inspiré du modèle suédois, le premier à être instauré, ces autorités se voient reconnaître des compétences et des pouvoirs fort similaires. Globalement, l'organe de contrôle veille au respect des dispositions de la législation, reçoit des plaintes et fait oeuvre de conciliateur, tient un registre des fichiers existants, procède à des vérifications et dénonce les infractions constatées. La réglementation anglaise est la plus extensive dans la définition des attributions de son *Data protection Register*. En R.F.A., les autorités de contrôle sont établies tantôt par une loi du *Bund* (contrôle du seul secteur public), tantôt par un acte normatif des *Länder* (contrôle du secteur public et du secteur privé).

En conclusion, bien que construites sur un schéma directeur identique, les législations européennes de protection des données personnelles révèlent en réalité des divergences sensibles quand on s'attache à en percevoir le contenu précis.

Cécile De Terwagne
Centre de Recherche Informatique et Droit
F.U.N.D.P. (Namur)

1 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, entrée en vigueur depuis 1985.

2 L'Espagne n'a pas de législation en la matière, mais elle a ratifié la Convention du Conseil de l'Europe et, aux termes de l'article 96 alinéa 1 de la Constitution espagnole, les conventions internationales valablement réalisées font partie de l'ordre juridique interne une fois publiées.
Quant à l'Italie, son gouvernement a présenté en 1984 un projet de loi répondant aux exigences de la convention de 1981, mais suite à de sévères critiques, émanant principalement de l'industrie, il l'a retiré.

3 Il en va de même dans la loi luxembourgeoise mais dans des circonstances plus particulières.

4 Il est à noter que la gratuité est la règle la plus répandue. Toutefois la Grande-Bretagne et l'Irlande soumettent pareil accès au paiement d'une somme, ce qui n'est pas sans importance si l'on sait qu'elle s'élève à 65 ECUS au Royaume-Uni et à 125 ECUS en Irlande.

«Autrement» publie

Info-révolution

L'ouvrage qui vous est présenté est le fruit d'une fabuleuse et large enquête menée en France, mais aussi en Europe et parfois au niveau mondial, auprès des principaux protagonistes des technologies de l'information et de la communication. Cela va des inventeurs, en passant par les fabricants, pour déboucher sur le simple utilisateur ou sur celui qui en ré-invente ou en pervertit les usages. De nombreux spécialistes ont été interrogés : technologues, économistes, sociologues, ingénieurs informaticiens et des télécommunications, spécialistes de l'audiovisuel, éducateurs, juristes et même *hackers*. Tous les secteurs d'activités ont été balayés. Enfin l'ensemble des approches, qu'elles soient sociale, géopolitique, culturelle, économique, a été pris en compte.

L'objectif est de sensibiliser les jeunes (quinze à vingt-cinq ans) et leurs prescripteurs, c'est-à-dire les professeurs d'histoire, de géographie, de technologie, d'économie, voire de français ou de mathématiques, aux technologies de l'information et de la communication - données alphanumériques, texte, son, visuel et audiovisuel -, ainsi que les animateurs socioculturels et les formateurs à cette réalité.

Extrait de la Revue «Autrement», série Mutations, n° 113, p. 13, mars 1990, prix 149 FF.